1. **需求分析**
   1. **项目背景和意义**

随着微机电系统技术的巨大进步，加上通信技术的发展，使得大规模的传感器网络使用越来越多。一个典型的传感器网络可能有几百到几百万个传感器节点。每个传感器节点通常是低成本的，计算和信息存储资源有限，高度的功率限制，并通过一个短距离的无线网络接口进行通信。这些特点确保了传感器网络的广泛应用，包括军事供应，环境监测和探索人迹罕至的环境等。与此同时，随着传感器网络的普及，针对物联网传感器等设备的安全攻击事件近年来不断攀升。主要攻击方式是利用设备漏洞获取设备控制权限，进而传播大规模恶意代码以控制网络空间，或利用漏洞窃取信息数据、劫持网络流量。

然而，根据Gartner在ITxpo2018的报告，到2021年物联网设备预计可达250亿个，市场相当庞大。与此同时，针对设备的攻击和安全事件也不断攀升，已严重威胁到用户的个人隐私甚至生命财产安全。在2018年的各种安全事件中，攻击对象已从简单的家用设备上升到工控、医疗、交通甚至航空航天领域，攻击类型涵盖利用僵尸网络实施的DDos攻击、利用网络摄像头破解实施的信息盗取等。物联网安全威胁已渗透至经济社会发展的多个层面，解决物联网安全问题刻不容缓。物联网攻击日益猖獗的重要原因在于，设备本身的安全设计存在严重缺陷。多数传感器设备生产商在设计和开发过程中，优先考虑实现功能以抢占市场而忽视安全因素，例如在开发阶段缺少对已存在漏洞的安全处理，在预交付阶段缺少安全测试等。在硬件方面，传感器设备资源受限，其接入网络后更难以实施安全配置与部署，而暴露于公网的传感器设备尤其易遭黑客攻击和利用。在操作系统方面，大量物联网设备对已有嵌入式系统进行了直接引用或简单二次开发，加剧了将已有漏洞带入系统的风险。

此外，传感器网络的安全问题似乎也没有得到充分考虑。尽管传感器网络的研究多基于应用场景，但在传统网络甚至是军事需求上应该得到更多关注。此外，由于硬件资源有限，通常使用的安全技术不能简单地应用于这一领域。随着技术的进步和相关研究的深入，传感器开始走向成熟。传感器网络的应用领域逐渐从军事开始向各行各业深入。比如我国在2015年9月公布的《中国制造业发展纲要(2015~2025)》中，就提出大力研究并推广物联网技术，使我国工业水平逐步达到“工业4.0”标准。而这些进步都必须依托传感器网络技术作为重要的基础。由于传感器通常部署在难以维护的环境中，除了普通网络面对的窃听攻击、拒绝服务攻击等攻击方式外，还面对着节点易被捕获和仿冒、传输的数据易被窃听和篡改等问题。在真正解决好这些问题之前，用户不可能轻易接受并部署一个安全和数据保护有问题的传感器网络。

本项目立足于与传感器安全建设需求，开展传感器安全检测平台的研究工作，借助这一平台，对各类实际环境中的传感器安全性进行试验，检验其抗网络攻击能力与抗漏洞利用能力，这将有助于改进传感器应用的安全性设计，增强传感器应用场景使用安全性。

* 1. **国内外现状**
     1. **传感器安全现状**

根据国家信息安全漏洞共享平台对2016年收录的物联网设备漏洞(含通用软硬件漏洞以及针对具体目标系统的事件型漏洞)进行了统计，物联网设备漏洞呈逐年增长趋势。根据阿里移动安全团队2015年统计，90%的物联网设备存在弱密钥、缓冲区溢出漏洞。近几年物联网传感器设备大量漏洞被相继披露。如：2013年黑帽大会上，Heffner展示多款网络摄像头的溢出类、口令硬编码、命令注入类漏洞，涉及到DLink、TPLink、Linksys、Trendnet设备厂商。攻击者利用这些漏洞可以进行非授权登入，劫持摄像头实时画面。此后各种类型的物联网传感器设备(小到智能家居，如智能灯泡、恒温器、路由器等，大到电动车、含有无线网络和娱乐系统的飞机)相继在黑客大会上被披露存在严重漏洞。此外，因安全漏洞引发的真实安全事件也层出不穷。2012年伊朗采用GPS干扰的方式俘获美国哨兵无人机。2016年10月21日，黑客利用大量被Mirai病毒感染的物联网传感器设备，发动针对Dyn管理的DNS服务器的DDoS攻击，影响范围涵盖美国东海岸、西海岸和欧洲部分地区，导致Twitter、GitHub、亚马逊、PayPal、BBC、华尔街日报等很多知名网站无法访问。总体来说，针对设备安全漏洞的攻击，不仅会造成隐私的泄露，更会造成财产的损失，严重的甚至会威胁到整个网络空间安全性。

综上，世界上的任何一个国家都不得不面对日益严峻的物联网传感器安全问题，其带来的严重后果不仅仅是经济损失那么简单，甚至会造成对现实世界的“硬摧毁”。因此，针对物联网传感器等设备的安全检测十分重要。

* + 1. **传感器固件安全技术现状**

针对物联网传感器设备漏洞能够成功攻击的原因，主要分为：(1)设备在设计和开发的过程中，主要考虑其功能性的实现，而在设计上忽略了安全性的考虑，在开发的过程中因疏忽引入漏洞，并且缺乏后期安全性的检查；(2)由于设备硬件资源受限，难以在设备上部署安全防护策略，导致漏洞更容易被攻击者利用。由于物联网传感器设备本身有对可移动、体积小的需求，导致第二个原因暂时无法克服。因此，最直接有效的方法是能够在投入使用前及时发现物联网设备中潜在漏洞。

物联网传感器设备存在大量未知漏洞，为设备自身以及网络空间带来了很多潜在的威胁。尽管政府部门和安全研究团队认识到设备自身漏洞带来的网络安全风险，以及加强对设备漏洞挖掘的迫切性，但目前仍缺少行之有效的物联网设备漏洞挖掘技术手段。市面上虽有较为丰富的关漏洞挖掘的技术、产品及研究团队，但大多是针对通用系统(Windows、Linux、Mac、Android)及其软件。

传感器是数据的采集入口，是物联网、智能工业、智能设备、无人驾驶等的“心脏”。工业环境对传感器的要求更高，在其精度、稳定性、抗震动和抗冲击性方面要求更为苛刻。工业传感器分为光电、热敏、气敏、力敏、磁敏、声敏、湿敏等不同类别。在物联网设备漏洞挖掘方面，由于不同厂商的设备在软硬件方面差异巨大、物联网设备源码、文档不公开等原因，难以构建物联网漏洞分析模型以及建立统一的动态仿真环境，难形成高效、自动化、批量化的物联网设备漏洞发现方法。目前传感器主要分为超声波传感器、红外线传感器、激光扫描仪、毫米波雷达以及立体视觉摄像头。因此，目前的物联网设备漏洞大多通过安全人员手工分析发现。

虽然通用平台的漏洞挖掘技术和工具不能完全适用于物联网设备，但大部分程序分析技术、安全测试思路和方案仍可用于物联网传感器设备。因此，设备漏洞挖掘技术仍然以通用程序分析和安全测试技术作为基础，结合设备特点，开展了相关漏洞挖掘技术的研究。

当前针对物联网固件的安全研究，多数是基于固件解压文件(包括二进制可执行文件、源码文件等)进行分析，并对新安全漏洞或新安全威胁进行挖掘。其中包括Thomas等采用静态分析方法挖掘硬编码类型的漏洞，通过提取函数特征并比对函数与静态数据进行建模识别，通过CFG程序控制流图确定数据比对的代码块影响力和重要度，以此评估函数重要性，在此基础上发现了硬编码的认证后门漏洞，并恢复SOAP、FTP协议指令集等。在后续研究中，Thomas等进一步采用了半监督学习方法，将二进制功能进行了分类，在语义描述的基础上识别后门，并成功挖掘到tenda设备后门。Davidson等使用KLEE符号执行引擎搭建工具FIE，使用一种符号化语言，建立行为的统一描述方式，并进行符号执行，通过内存污染等方法提升分析覆盖率和准确性，可挖掘到内存破坏和外网IO误用类的漏洞。但由于该工具依托符号执行，需获取固件源码，且执行环境与真实环境存在差异，因此可能出现误报。此外，符号执行存在路径爆炸问题，使其应用受到进一步限制。

综上，对于固件安全随着物联网传感器的广泛应用，越来越多的安全机构从事固件安全评估的研究探索工作。可以利用静态分析技术、动态分析技术、同源性分析技术等对传感器固件安全进行进一步深入研究，借以研发传感器固件安全检测技术。

* + 1. **传感器网络安全技术现状**

网随着传感器技术、嵌入式技术、分布式信息处理技术的发展,以大量的具有微处理能力的微型传感器节点组成的传感器网络使得我们对各种环境下一体化信息的有效获取成为可能。传感器网络是由大量体积小具有通信和监测能力的传感器节点组成。这些节点被稠密部署在监测区域，以达到监测物理世界的目的。与传统的通讯网络和移动网络相比,传感器网络具有自组织性、低成本性、资源受限和以数据为中心等特点,这些特点使得传感器网络在恶劣地方进行大规模部署信息获取网络成为可能。值得指出的是,传感器网络也可以在智能家庭、厂房监控等进行小规模的部署,传感器节点数量可能是几个到几十个,传感器节点也可能是昂贵的,资源不受限制等等。这种多样性的特点使得对传感器网络的研究大多以应用为导向展开研究。

保障传感器网络的安全运行是传感器网络得以广泛应用的基础之一。事实上、缺乏有效的安全机制已经成为传感器网络应用的主要障碍。尽管在传感器网络安全技术研究方面已经取得了较大的成绩，许多传感器网络安全技术已经被提议，但是由于在传感器网络协议设计阶段，没有考虑安全问题，因此没有形成完善的安全体系，传感器网络存在着巨大的安全隐患。与传统的网络不同,传感器网络本身的特点决定了其安全研究的复杂性和独特性如传感器节点大规模地分布在未保护或敌对环境中,节点容易被捕获而泄漏敏感信息；昂贵的安全机制不能适用于资源受限的传感器网络；通信的特性使得窃听、干扰等攻击更加容易；另外,传感器节点的低成本也使得节点被捕俘后容易泄露密钥,从而导致整个网络的安全受到威胁。

传感器网络安全技术研究和传统网络有着较大区别，但是他们的出发点都是相同的，均需要解决信息的机密性、完整性、消息认证、组播/广播认证、信息新鲜度、入侵监测以及访问控制等问题。传感器网络的自身特点（受限的计算、通信、存储能力，缺乏节点部署的先验知识，部署区域的物理安全无法保证以及网络拓扑结构动态变化等）使得非对称密码体制难以直接应用，实现传感器网络安全存在着巨大的挑战。不断有新的基于传感器网络的安全技术提出，但仍待实际应用验证。

综上，传感器网络的不断增长，各国都在积极研究探索如何构建高效安全的传感器网络，传感器网络相关技术的提升与传感器网络方面的安全研究的不断深入，都为传感器网络安全进行进一步深入研究提供了新的思路，可以借以研发传感器网络安全检测技术。